(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property
Organization
International Bureau

(43) International Publication Date
23 December 2004 (23.12.2004)

PCT

(10) International Publication Number
WO 2004/112306 A3

(51) International Patent Classification⁷: G06F 7/72

(21) International Application Number: PCT/IB2004/050813

(22) International Filing Date: 1 June 2004 (01.06.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
03101718.9 12 June 2003 (12.06.2003) EP

(71) Applicant *(for DE only)*: **PHILIPS INTELLECTUAL PROPERTY & STANDARDS GMBH** [DE/DE]; Steindamm 94, 20099 Hamburg (DE).

(71) Applicant *(for all designated States except DE, US)*: **KONINKLIJKE PHILIPS ELECTRONICS N. V.** [NL/NL]; Groenewoudseweg 1, NL-5621 BA Eindhoven (NL).

(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: **AVANZI, Roberto** [IT/DE]; c/o Philips Intellectual Property &, Standards GmbH Weisshausstr. 2, 52066 Aachen (DE).

(74) Agent: **MEYER, Michael**; Philips Intellectual Property &, Standards GmbH Weisshausstr. 2, 52066 Aachen (DE).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

(88) Date of publication of the international search report: 10 February 2005

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: METHOD FOR DEFENCE AGAINST DIFFERENTIAL POWER ANALYSIS ATTACKS

$$\begin{tikzcd}
\mathcal{J}(C)(\mathbb{K}) \arrow[r, "\times n"] \arrow[d, "\phi"'] & \mathcal{J}(C)(\mathbb{K}) \\
\mathcal{J}(\tilde{C})(\mathbb{K}) \arrow[r, "\times n"'] & \mathcal{J}(\tilde{C})(\mathbb{K}) \arrow[u, "\phi^{-1}"']
\end{tikzcd}$$

(57) **Abstract:** In order to refine a method for defence against at least one attack made by means of differential power analysis on at least one hyperelliptic cryptosystem, in particular at least one hyperelliptic public key cryptosystem, which is given by at least one hyperelliptic curve (C) of any genus (g) over a finite field (K) in a first group, where the hyperelliptic curve (C) is given by at least one co-efficient, so that an essential contribution can be made towards an efficient and secure implementation of the hyperelliptic cryptosystem, it is proposed that the hyperelliptic curve (C) and/or at least one element of the first group, in particular at least one in particular reduced divisor and/or at least one intermediate result of a scalar multiplication, is randomised.

WO 2004/112306 A3

INTERNATIONAL SEARCH REPORT

PCT/IB2004/050813

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F7/72

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	JOYE M ET AL: "PROTECTIONS AGAINST DIFFERENTIAL ANALYSIS FOR ELLIPTIC CURVE CRYTOGRAPHY - AN ALGEBRAIC APPROACH -" CRYPTOGRAPHIC HARDWARE AND EMBEDDED SYSTEMS. 3RD INTERNATIONAL WORKSHOP, CHES 2001, PARIS, FRANCCE, MAY 14 - 16, 2001 PROCEEDINGS, LECTURE NOTES IN COMPUTER SCIENCE, BERLIN : SPRINGER, DE, vol. VOL. 2162, 14 May 2001 (2001-05-14), pages 377-390, XP008002642 ISBN: 3-540-42521-7 cited in the application section 4 ----- -/--	1,3,4, 7-10

☒ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search 23 November 2004	Date of mailing of the international search report 21/12/2004
Name and mailing address of the ISA European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Authorized officer Verhoof, P

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CORON J-S: "RESISTANCE AGAINST DIFFERENTIAL POWER ANALYSIS FOR ELLIPTIC CURVE CRYPTOSYSTEMS" CRYPTOGRAPHIC HARDWARE AND EMBEDDED SYSTEMS. INTERNATIONAL WORKSHOP, XX, XX, August 1999 (1999-08), pages 292-302, XP000952243 page 301, line 1 - line 17	1,2,5-10
A	T. LANGE: "Weighted Coordinates on Genus 2 Hyperelliptic Curves" INTERNET ARTICLE, 'Online! 11 October 2002 (2002-10-11), XP002306887 Retrieved from the Internet: URL:http://www.itsc.ruhr-uni-bochum.de/tanja/preprints/jac_sub.ps.gz> 'retrieved on 2004-11-15! cited in the application page 2 - page 3	5,6
A	DE 100 57 203 C (CV CRYPTOVISION GMBH) 6 June 2002 (2002-06-06) paragraph '0023!	1-10
T	CANTOR D G: "COMPUTING IN THE JACOBIAN OF A HYPERELLIPTIC CURVE" MATHEMATICS OF COMPUTATION, AMERICAN MATHEMATICAL SOCIETY, US, vol. 48, no. 177, 1987, pages 95-101, XP000909603 the whole document	1-10
T	LOCKHART P: "ON THE DISCRIMINANT OF A HYPERELLIPTIC CURVE" TRANSACTIONS OF THE AMERICAN MATHEMATICAL SOCIETY, AMERICAN MATHEMATICAL SOCIETY, PROVIDENCE, RI, US, vol. 342, no. 2, April 1994 (1994-04), pages 729-752, XP008038424 ISSN: 0002-9947 the whole document	1-10
T	MENEZES A J ET AL: "APPENDIX AN ELEMENTARY INTRODUCTION TO HYPERELLIPTIC CURVES" ALGEBRAIC ASPECTS OF CRYPTOGRAPHY, XX, XX, 1998, pages 155-178, XP000987354	1-10

INTERNATIONAL SEARCH REPORT

PCT/IB2004/050813

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
DE 10057203 C	06-06-2002	DE 10057203 C1	06-06-2002